Gordon L. Gibby MD
KX4Z
15216 NW 41st Avenue
Newberry FL 32669

April 6 2019

Dear Sirs:

I am a medical doctor, not a Professor of Engineering, but I do have two degrees in Electrical Engineering and I simply don't understand comments made by Prof. Ted Rappaport PhD in regards to his support of RM-11831. (See: https://ecfsapi.fcc.gov/file/1040322516387/FCC Letter RM 11831 final.pdf dated April 3 2019.)

In his filed comments on NYU Wireless letterhead, the Professor states,

> *"RM-11831 importantly also assures national security by providing transparency and self-monitoring by the public of all amateur radio transmissions in the HF spectrum that routinely cross international borders. "*

A quick initial point; It is not clear to me how RM-11831 would arrange for the monitoring of **ALL** amateur radio radio transmissions in the HF spectrum, by the public. That would appear to be a very large task! How does this Petition arrange for such 24/365 coverage all every amateur radio signal in the HF spectrum? But perhaps this was a simple semantic error.

I then note that the Professor often uses the phrase "effectively-encrypted": (emphases added by me)

> *"d) which are currently used to send illegal point-to-point private email and **effectively-encrypted** files while operating on the US amateur radio HF spectrum."*
>
> And
>
> *"RM-11831 cures the existing problem of **effectively-encrypted** and proprietary ARQ traffic (including Pactor 3 and other modes like WINMOR, STANAG, ARDOP) that cannot be intercepted over the air by other ham operators or the FCC "*

But later in he calls it "obscured":

> *"the major problems of **obscured** point-to-point email traffic"*

The use of the word "obscured" must be taken seriously, since 97.113(a) (4) makes that unlawful:

> *(4) Music using a phone emission except as specifically provided elsewhere in this section; communications intended to facilitate a criminal act; messages encoded for the purpose of*

obscuring their meaning, except as otherwise provided herein; obscene or indecent words or language; or false or deceptive messages, signals or identification.

And thus the Professor is alleging illegal actions ongoing with no action by the FCC for almost decades…. Capture of which would actually require

"specialized 'signal intelligence' equipment at the FCC, "

These astonishing claims are fascinating given the well-known facts about PACTOR and WINLINK communications:

- Pactor II is technically specified here:
  https://www.p4dragon.com/download/PACTOR-2 Protocol.pdf

- Pactor III is technically specified here:
  https://www.p4dragon.com/download/PACTOR-3 Protocol.pdf

- WINLINK B2F structure is documented here:
  https://www.winlink.org/B2F

- and free source code for the latter is provided here:
  https://github.com/ARSFI/Winlink-Compression

- and the Petitioner himself was kind enough to point to this second-source firm which produces software which can decode PACTOR signals:

  https://www.comintconsulting.com/krypto500

  in his helpful post #156 at https://forums.qrz.com/index.php?threads/new-digital-petition-at-the-fcc-rm-11831.652589/page-16

I would presume that the known technical expert Dr Rappaport is quite well aware of all of the above facts. That likely explains why he does not call this an "*encrypted*" system, but does not why he calls it the more legally-serious "*obscured*" mode.

However what really puzzles me is why the Petitioner and Dr. Rappaport have gone to such great lengths to attempt to prevent PACTOR II/III and WINLINK communications, rather than just providing the very answer which they so desperately demand over and over? A decoder!

Surely with publicly available hardware from SCS, and publicly available compression algorithms, marrying the two and providing full real-time monitoring of PACTOR and/or WINLINK would be quite a simple project! It might not even rise to the level of a Master's Thesis for one of Dr.

Rappaport's students – but it might make a nice undergraduate project for an Electrical Engineer or a Computer Science major.

Why has this not yet be done, if this is so important to the defense of the nation, the defense of the amateur waves, and the security of our people?

Further, I'm told there exists underground code to decipher these proprietary modes, and since they are published, it would seem to be a great doctoral thesis for one of Dr. Rappaport's students to reproduce them from the Technical Specifications published openly and compare their efficacy to the commercially available system on the market for such a long time.

I understand that some of these protocols have been in use since 2002, and if so patently illegal as the Petition and the Commenter allege, how do they explain that the FCC has not put a stop to this, and the ITU has actually helped install new gateways for this very system? (See: https://winlink.org/sites/default/files/itu_continues_strengthening_emergency_telecommunications_in_the_americas-converted.pdf)

These facts puzzle me. And make me believe that RM-11831 is not supported by true need or facts.

Sincerely,

Gordon L. Gibby MD
KX4Z